REMARKS

The specification has been amended to replace the attorney docket number with the patent application serial number of the cited application.

Claims 1, 27 have been amended. Support for the amendment of Claims 1, 27 appears in the specification at least at page 16, line 9 to page 17, line 10.

Claims 5, 28 have been amended. Support for the amendment of Claims 5, 28 appears in the specification at least at page 10, lines 14-20.

Claim 16 has been amended to incorporate features of Claims 17-18, which accordingly have been canceled without prejudice. Claims 19-20 have been amended to depend from Claim 16. Claim 29 has been amended similarly to Claim 16.

New Claims 30-33 have been added. Support for Claim 30 appears in the specification at least at page 16, lines 13-16. Support for Claim 31 appears in the specification at least at page 8, lines 19-20. Support for Claims 32-33 appears in the specification at least at page 9, line 32 to page 10, line 5. Claim 30, which depends from Claim 1, is allowable for at least the same reasons as Claim 1. Claims 31-33, which depend from Claim 5, are allowable for at least the same reasons as Claim 5.

Request for Examiner Interview.

Should the Examiner be of the opinion that this Amendment does not place the application in a condition for allowance, Applicant hereby requests an Examiner Interview prior to the issuance of the next communication from the USPTO to expedite prosecution.

Claims 1-16, 19-29 are novel over Magdych et al. (6,546,493).

The Examiner states:

As per claim 1; "A method comprising: …

> extracting a malicious code signature from said malicious code [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 3,lines 23-49, whereas the comparison of 'a plurality of virus/attack signatures … **or extract the harmful information from the infected communications** …' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];
> creating an extracted malicious code packet including said malicious code signature [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., separate intrusion/attack detection (first computer) system versus the risk assessment/remediation (second computer) system **where the first to second extracted malicious code information clearly is transferred in a coded packet**), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; …(Office Action, pages 2-3, emphasis added.)

The Examiner's statement is respectfully traversed. As set forth further below, Magdych et al. teaches: 1) network communications **between** networked devices are scanned; and 2) harmful information from an infected communication is **extracted to disinfect the communication**.

More particularly, Magdych et al. teaches:

> … The intrusion detection tool 112 detects attacks or intrusions by **scanning network communications between the various foregoing network devices**. Of course, the intrusion detection tool 112 may also be capable of scanning executable files, application macro files, disk boot sectors, etc. This scanning may include comparing the network communications, etc. with a plurality of virus/attack signatures, known vulnerabilities and/or policies that may be constantly updated. Upon the detection of any of these by the intrusion detection tool 112, a remedying event may then be used to execute a risk assessment scan, report the problem, quarantine the infected communications, and/or **extract the harmful information from the infected communications**, thereby **disinfecting the communications**. (Col. 3, lines 35-48, emphasis added.)

For at least the above reasons, Magdych et al. does not teach or suggest:

> A method comprising:
> detecting an attack by malicious code on a first computer system;
> extracting a malicious code signature from said malicious code comprising:
> **locating a caller's address of said malicious code in a memory of said first computer system**; and
> **extracting a specific number of bytes backwards from said caller's address**;
> **creating an extracted malicious code packet including said malicious code signature**; and
> sending said extracted malicious code packet from said first computer system to a second computer system,

as recited in amended Claim 1, emphasis added. As set forth in MPEP 2131, Eighth Edition, Rev. 5, August 2006 at page 2100-67:

> TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM

For at least the above reasons, Claim 1 is allowable over Magdych et al.

Claims 2-4, which depend from Claim 1, are allowable for at least the same reasons as Claim 1. Claim 27 is allowable for reasons similar to Claim 1.

For similar reasons, Magdych et al. does not teach or suggest:

> A method comprising:
> detecting an attack by malicious code on a first computer system;
> **creating an extracted malicious code packet including parameters associated with said malicious code**, said parameters being selected from the group consisting of a **caller's address of said malicious code in a memory of said first computer system**, a name of a process in which said attack took place, ports connected to said process, service pack levels,

> operating system information, patch level information, and combinations thereof; and
>
> sending said extracted malicious code packet from said first computer system to a second computer system,

as recited in amended Claim 5, emphasis added. Claims 6-15, which depend from Claim 5, are allowable for at least the same reasons as Claim 5. Claim 28 is allowable for reasons similar to Claim 5.

Claim 16 has been amended to incorporate features of Claim 18. Accordingly, the rejection of Claim 18 shall be discussed as applied to amended Claim 16.

The Examiner states:

> Claim 18 ***additionally recites*** the limitations that; "The method of Claim 17 wherein said signature update is delivered to an intrusion detection system.".
>
> The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 2,lines 27-55, whereas the comparison of '… **a database on known vulnerabilities may then be updated [i.e., at the 'intrusion detection system'] based on risk assessment scan …**' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations. (Office Action, pages 15-16.)

Accordingly, Magdych et al. teaches a feedback mechanism between the risk assessment scanning tool 110 and the intrusion detection tool 112. Specifically, Magdych et al. teaches:

> Once complete, the results in the form of any additional known vulnerabilities are outputted in operation 510. As an option, the results may be used to update the database of threats (i.e. vulnerabilities and polices) mentioned hereinabove in operation 302 of FIG. 3. Note operation 512. As such, fixture use of such database by the intrusion detection tool 112 may include the known vulnerabilities outputted in operation 510. Thus, **there is a feedback mechanism between the risk assessment scanning tool 110 and**

> **intrusion detection tool 112**. (Col. 7, lines 1-10, emphasis added.)

For at least the above reasons, Magdych et al. does not teach or suggest:

> A method comprising:
> receiving an **extracted malicious code packet from a first computer system** with a second computer system, **said first computer system being a host computer system and said second computer system being a local analysis center computer system**; and
> determining whether an attack threshold has been exceeded based upon said extracted malicious code packet, wherein upon a determination that an attack threshold has been exceeded, said method further comprising **delivering a signature update comprising a malicious code signature to an intrusion detection system**,

as recited in amended Claim 16, emphasis added. Accordingly, Claim 16 is allowable over Magdych et al. Claims 19-26, which depend from Claim 16, are allowable for at least the same reasons as Claim 16. Claim 29 is allowable for reasons similar to Claim 16.

For at least the above reasons, Applicant respectfully requests reconsideration and withdrawal of this rejection.

Conclusion.

Claims 1-16, 19-33 are pending in the application. For the foregoing reasons, Applicant respectfully requests allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 31, 2007.

Attorney for Applicant(s)

May 31, 2007
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
Tel.: (831) 655-0880